Bilişim Suçu Nedir?

Bilişim teknolojinin yardımı ile (genellikle sanal ortamda) kişi veya kurumlara maddi veya manevi zarar vermek, suç işlemek.

Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenen suçlardır

Hangi Suçlar Bilişim Suçudur?

1. **E-POSTA ELE GEÇİRME**

Bir kişiye ait e-posta veya kullanıcı bilgilerini ele geçirmek, değiştirmek veya silmek.

2. **KULLANICI HESAPLARI İLE İLGİLİ SUÇLAR**

Bir kişi veya kurum adına sahte e-posta / profil / hesap oluşturmak. Bu sahte hesapları kullanarak çeşitli paylaşımlar yapmak.

3. **WEB SAYFALARI KULLANILARAK İŞLENEN SUÇLAR**

Sahte alışveriş siteleri kurarak kullanıcıları dolandırmak.

Devlet karşıtı gruplara ait içerikleri yayınlamak / paylaşmak.

İnternetten alışverişte kullanıcıların kredi kartı bilgilerini ele geçirmek.

4. **BİLGİSAYARI VEYA BİLGİLERİ ELE GEÇİREREK İŞLENEN SUÇLAR**

Başkasına ait bilgisayara, ağa veya sisteme izinsiz girmek, bilgileri kopyalamak, silmek veya değiştirmek.

5. **LİSANSIZ YAZILIM VE İÇERİKLERİN KULLANIMI İLE İLGİLİ SUÇLAR**

Telif hakkı ile korunan yazılım, dosya, resim, fotoğraf, müzik, video klip ve film dosyalarını izinsiz indirmek, paylaşmak, tamamını veya bir kısmını kullanmak.

6. **ÇEVRİMİÇİ İLETİŞİM SIRASINDA İŞLENEN SUÇLAR**

Sosyal ağlar, sohbet siteleri, forumlar gibi kullanıcıların birbirleriyle iletişim kurdukları sitelerde kişi ya da kuruluşa hakaret, küfür etmek veya aşağılayıcı ifadeler kullanmak.

7. **KREDİ KARTI, KONTÖR/TL DOLANDIRICILIĞI**

Telefon, e-posta ve çeşitli iletişim araçları kullanarak kişilerden kredi kartı bilgileri istemek.

Tehdit veya şantaj yoluyla çeşitli hesaplara TL veya kontör yüklenmesini istemek.

BİLİŞİM SUÇLARINA KARŞI ALINABİLECEK TEDBİRLER NELERDİR?

 Lisanssız yazılımlar ve içerikler (müzik, resim, fotoğraf video vs.) kullanmayın.

 Çeşitli yollarla kırılmış, içeriği değiştirilmiş veya güvenilir olmayan yazılımlar yüklemeyin.

 Bilgisayar sistemini korumaya yönelik anti-virüs, güvenlik duvarı gibi yazılımlar kullanın ve mümkün olduğunca güncellemelerini yapın.

 Kullanılan yazılımların en güncel ve sorunsuz sürümlerini temin etmeye çalışın.

 Telefon, e-posta vs. gibi yollarla sizden kişisel bilgilerinizi (ad, soyad, adres, telefon gibi), parolanızı ya da kredi kartı şifrenizi isteyenlere itibar etmeyin.

 İnternet ortamında tanımadığınız veya şüphelendiğiniz kişilere kişisel ve özel bilgilerinizi vermeyin!

 Sosyal ağlarda, forum ve sohbet yazılımlarında kişi veya kurumlara karşı küfür, hakaret veya aşağılayıcı sözler kullanmayın. Türkçe'mizi en güzel şekilde kullanmaya çalışın.

 Kimsenin e-posta ve çeşitli hesaplarına (facebook, twitter vs.) giriş yapmaya, şifresini tahmin etme yoluyla ele geçirmeye çalışmayın!

 Sahte hesaplar oluşturmayın ve bu hesapları kullanarak paylaşımlar yapmayın!

 Başkasına ait bilgisayarı, interneti ve ağları izinsiz olarak kullanmayın, bilgileri silmeyin, değiştirmeyin veya kopyalamayın! Kişisel Şifreler İle İlgili Öneriler

 Kişisel şifrelerini kesinlikle en yakınınız olsa dahi kimse ile paylaşmayın! Tüm hesaplarınızda aynı şifreyi kullanmayın.

Güvenli Şifre Oluşturma

 Şifrelerinizde kişisel bilgilerinize yer vermeyin. Örneğin, adınız, doğum tarihiniz veya kimlik numaranız. Örneğin, ali1999, 32423526655, 1986 gibi

 Şifrenizde ardışık sayılar, harfler kullanmayın. Örneğin, 123456, 1234, abcd gibi.

 Tahmin edilmesi kolay yanyana bulunan tuşları kullanmayın. Örneğin, qwerty, asdf gibi.

 Şifreniz en az 8 basamaklı olsun.

 Mümkün olduğunda aşağıdaki karakterlerden içersin.

 Büyük/küçük harf (A,a…Z,z) Rakam (0-9)

 Noktalama (.,; gibi) Özel karakter (-!+ gibi)